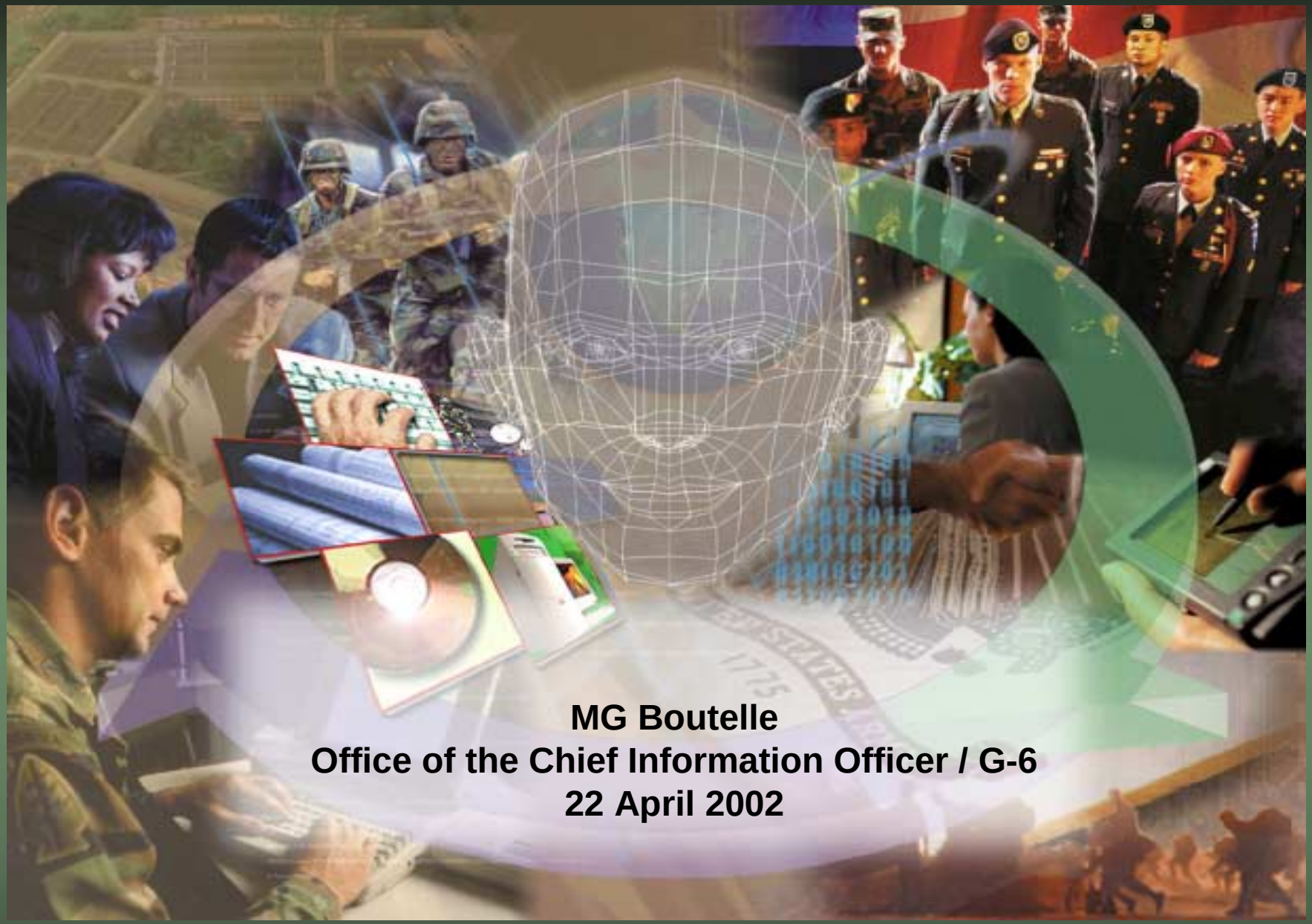
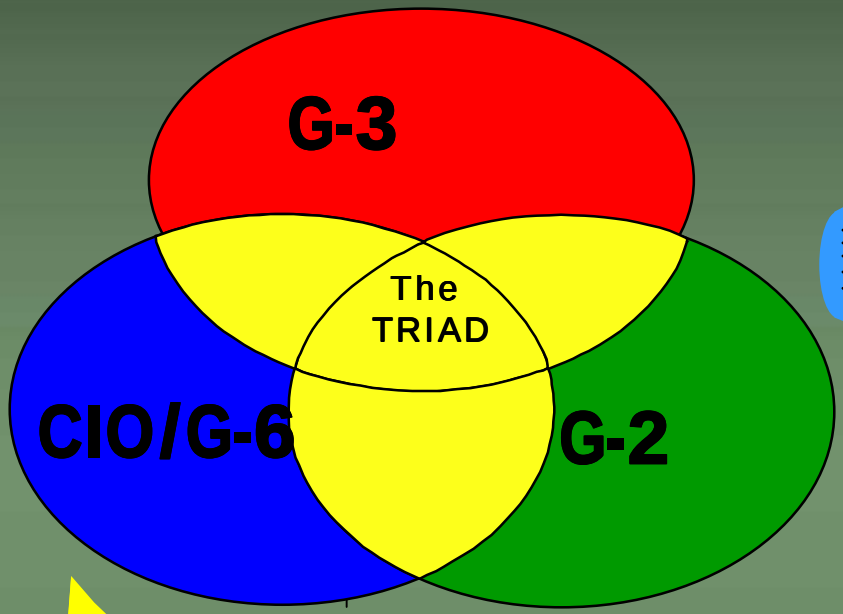
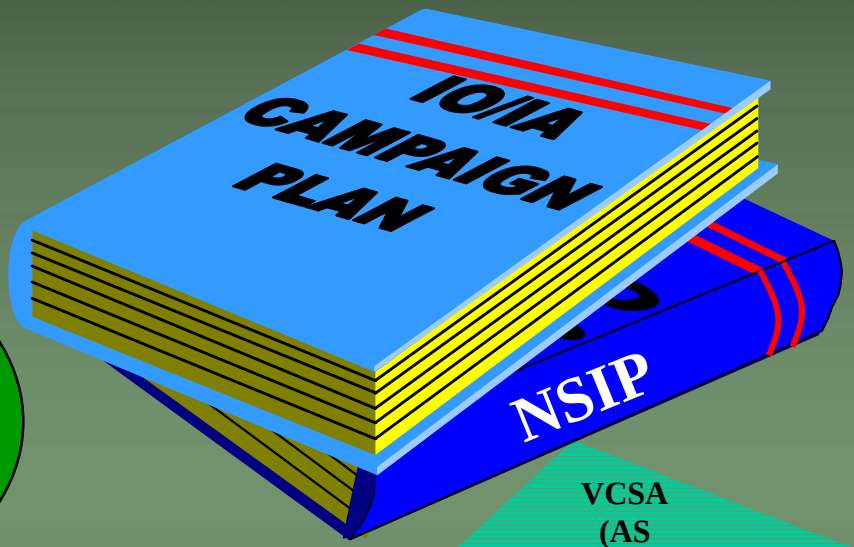


MG Boutelle
Office of the Chief Information Officer / G-6
22 April 2002

Army Information Assurance
The Policy Making Process





Input from Leadership and Field

VCSA (AS REQUIRED)

SENIOR IO REVIEW COUNCIL

GOSC

COUNCIL OF COLONELS

Information Operations (Responsibilities)

The G-2 provides the intelligence support and some operational capabilities.

C2 Attack.

The G-6 is the Army's CIO, and provides the foundation of Information Assurance policies.

C2 Protect.

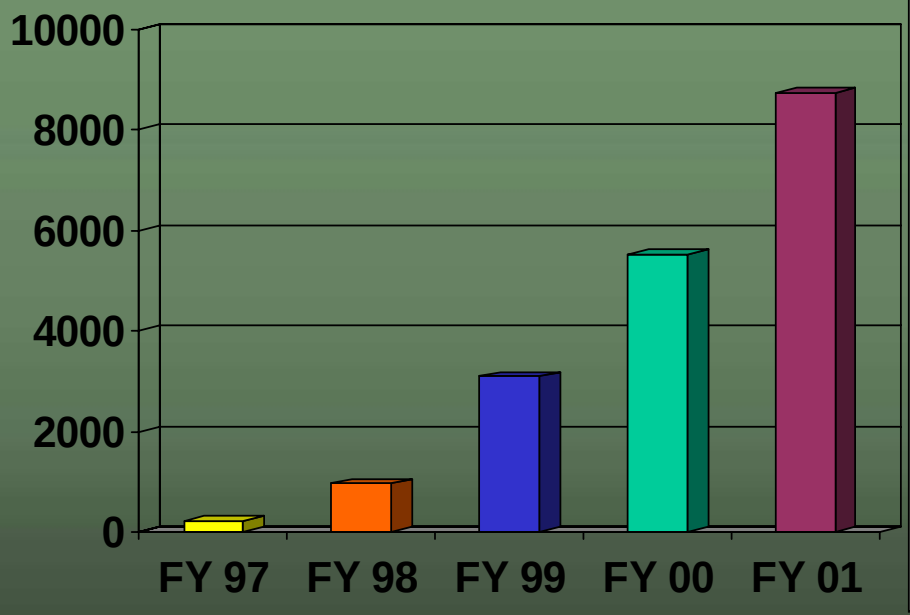
- **The G-3 is the <u>Army's IO lead</u>, and has OPCON of the Army's full spectrum, IO field deployable force.**

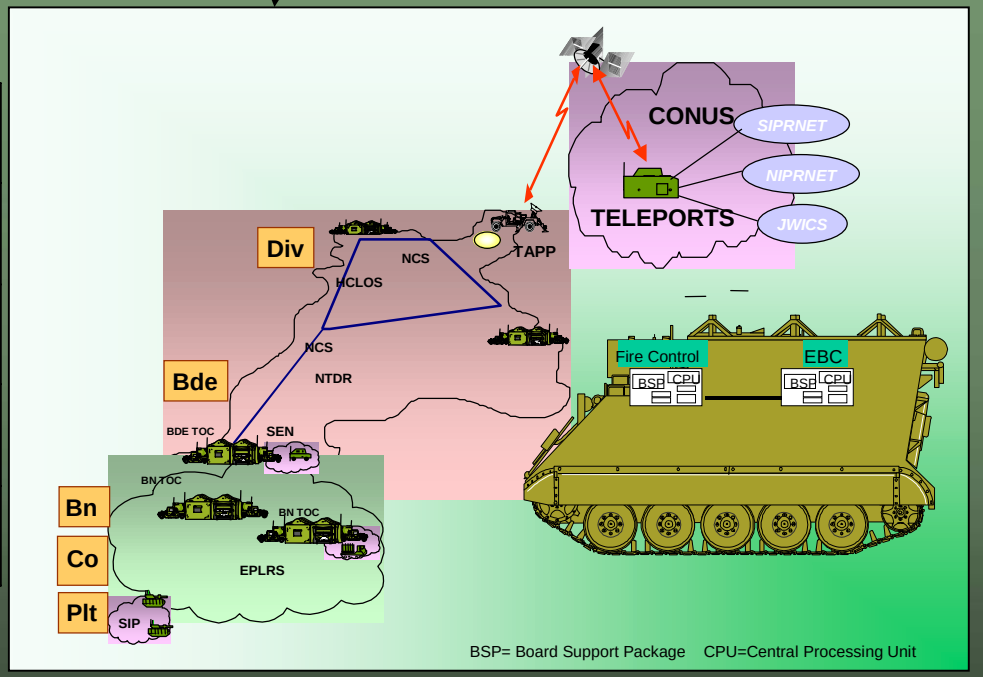
Civil Affairs and Public Affairs.

The Threat Environment

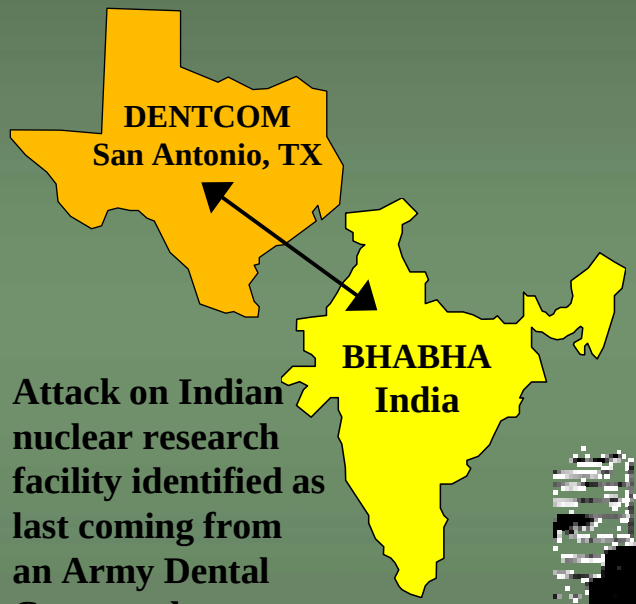
Insiders
Terrorists
Script-kiddies
Hackers
State Sponsorship

Multiple Sources
Growing Rapidly
Potentially devastating

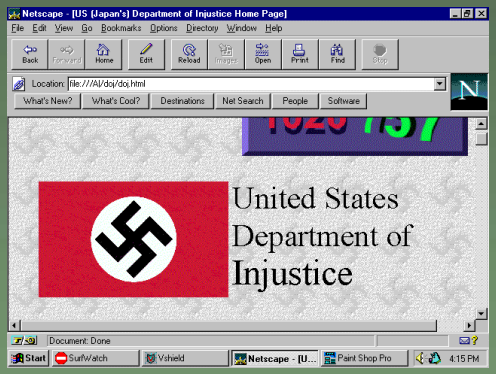




CONSEQUENCES OF BEING VULNERABLE TO THE THREAT



Attack on Indian nuclear research facility identified as last coming from an Army Dental Command system



Loss of Public Confidence

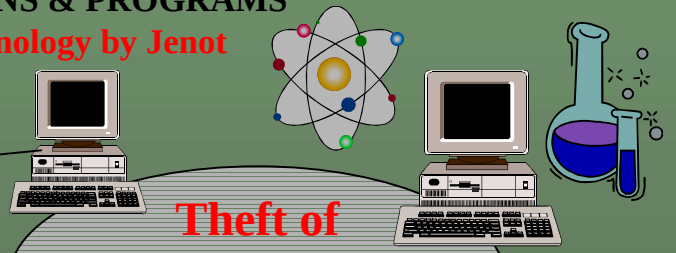
e.g., apparent inability to protect publicly accessible web sites

Unprotected Backdoor into network

Intruder able to search files at will, control the Command's network, and potentially *control the Commander's C2*

STOLEN PLANS & PROGRAMS
MSE Technology by Jenot

RESEARCH LABORATORIES

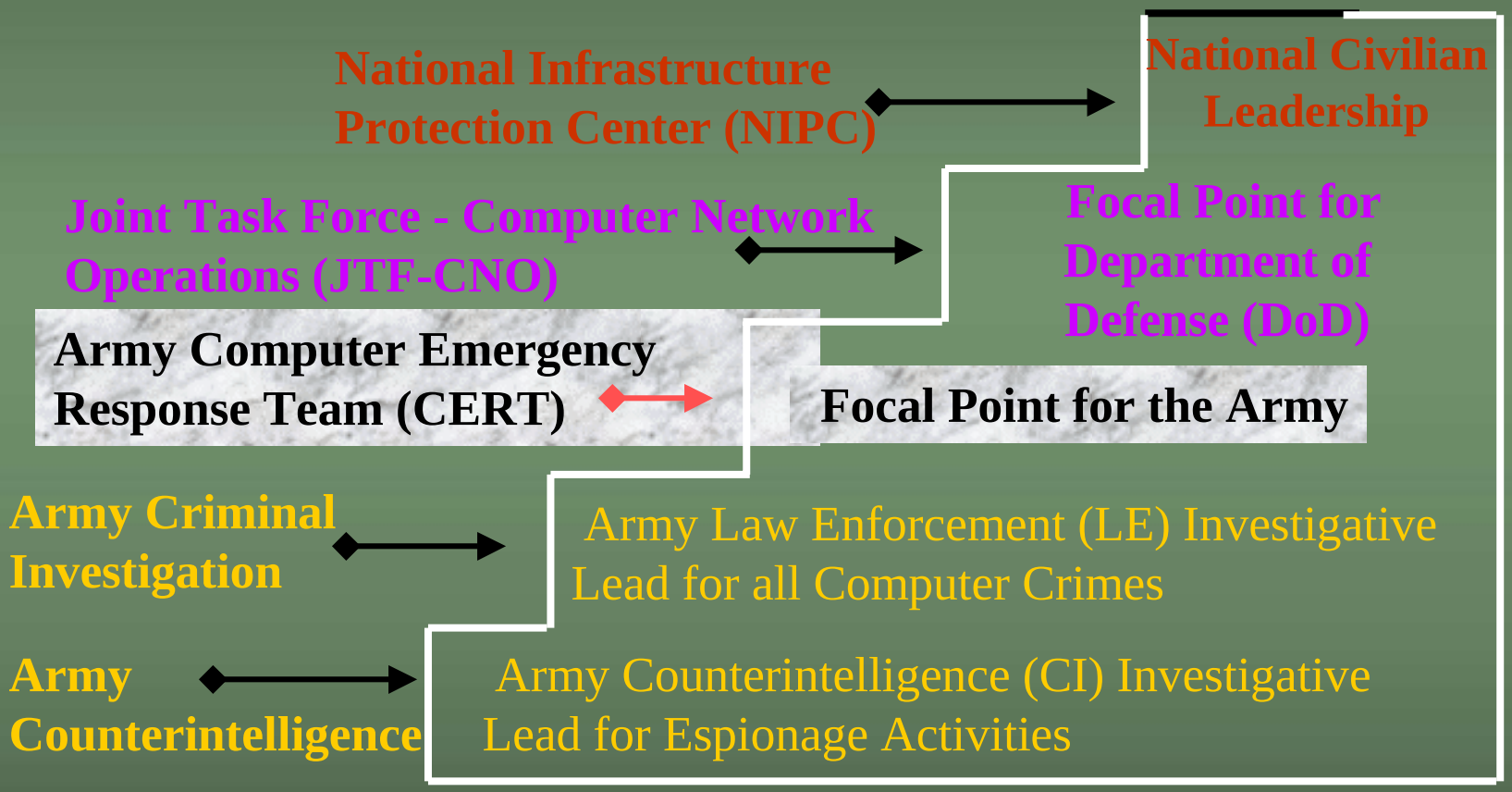


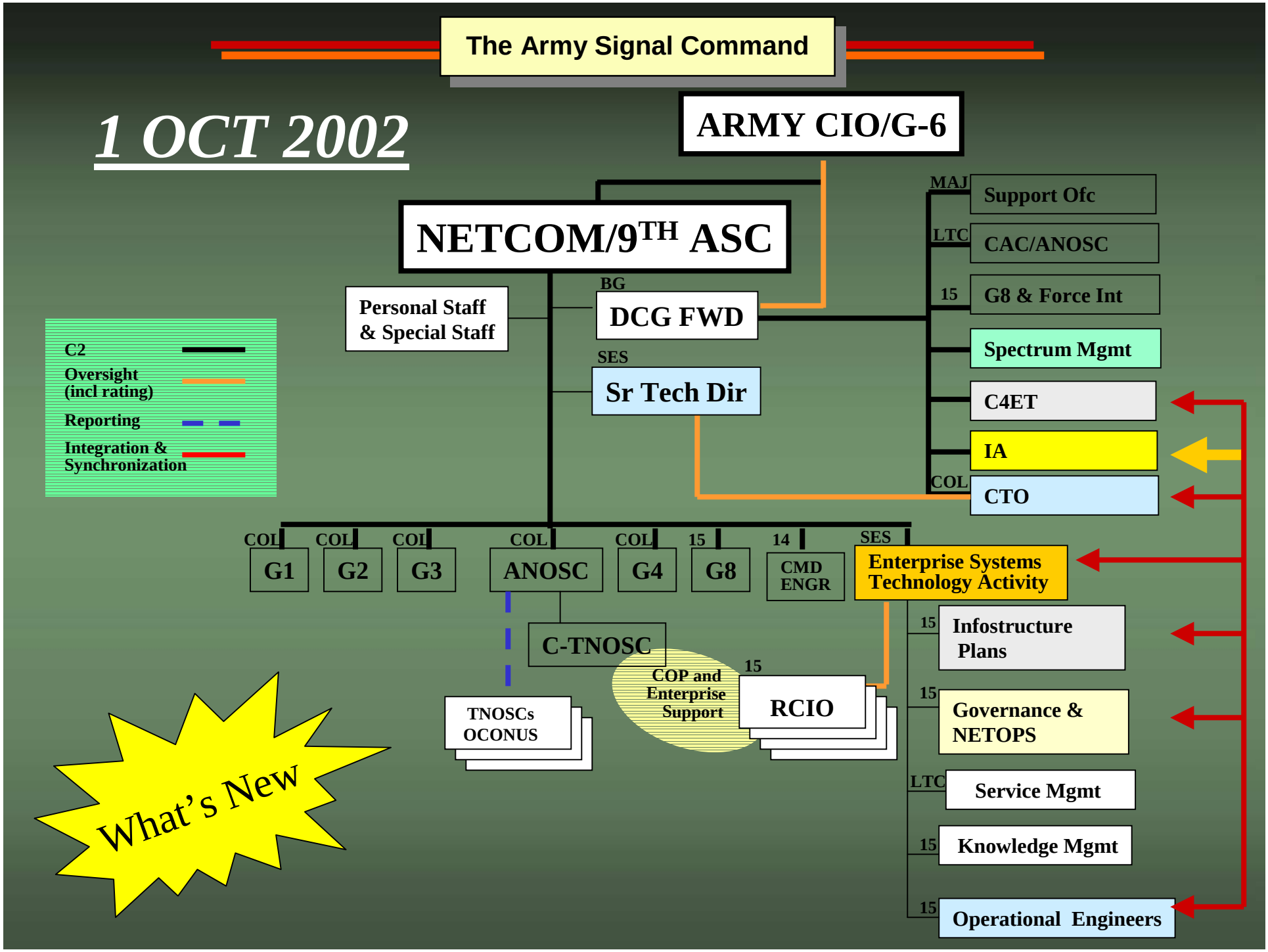
Theft of Information, System Disruption/Denial

FINANCIAL DATA
$1 Trillion in Cyberspace at any given time in a year

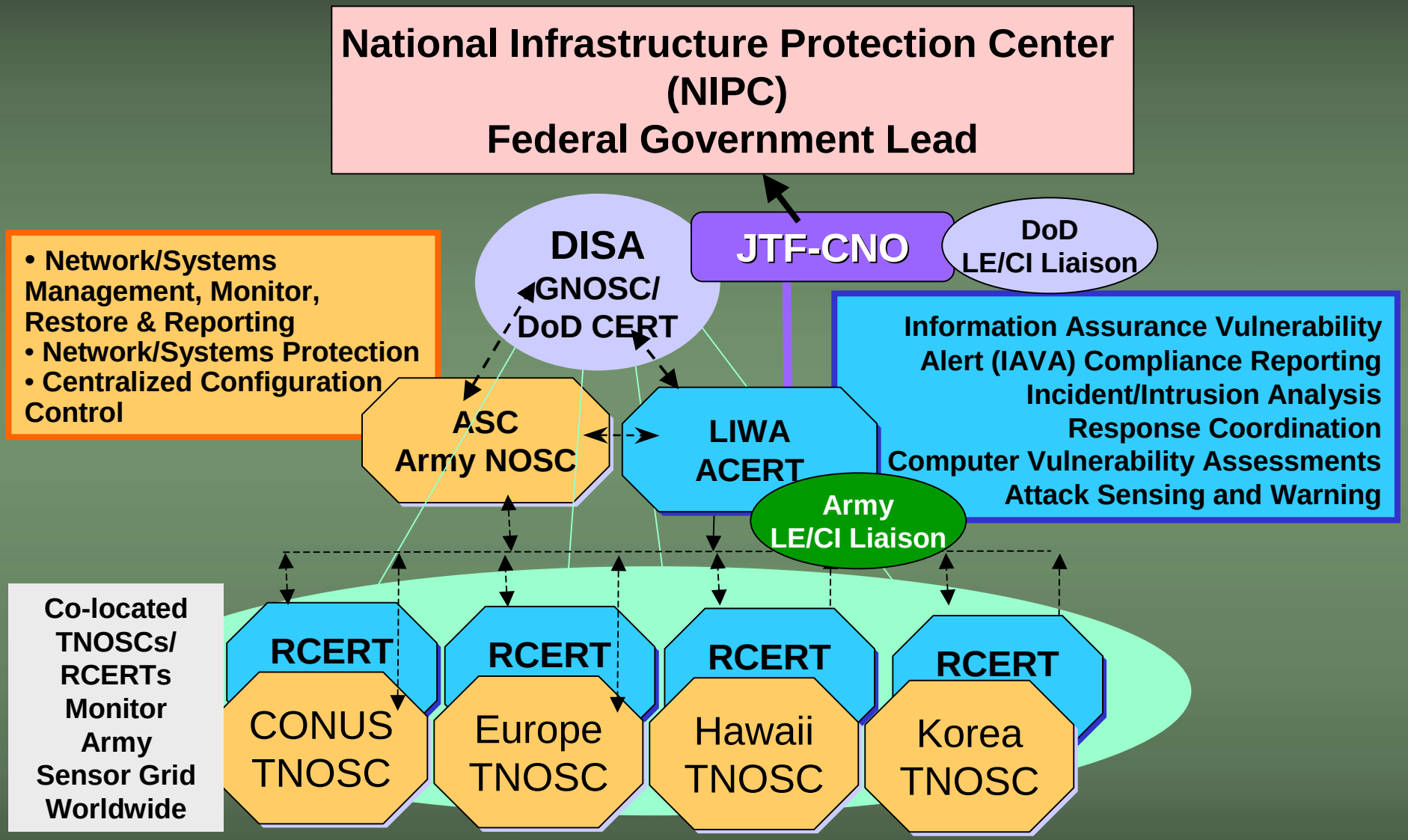
Potential International Repercussions

Computer Network Defense (CND)
The Participants




The Army Signal Command
1 OCT 2002
ARMY CIO/G-6
NETCOM/9TH ASC
Personal Staff & Special Staff
BG
DCG FWD
SES
Sr Tech Dir
C2
Oversight (incl rating)
Reporting
Integration & Synchronization
MAJ
Support Ofc
LTC
CAC/ANOSC
15
G8 & Force Int
Spectrum Mgmt
C4ET
IA
COL
CTO
COL
G1
COL
G2
COL
G3
COL
ANOSC
COL
G4
15
G8
14
CMD ENGR
SES
Enterprise Systems Technology Activity
C-TNOSC
TNOSCs OCONUS
COP and Enterprise Support
15
RCIO
15
Infostructure Plans
15
Governance & NETOPS
LTC
Service Mgmt
15
Knowledge Mgmt
15
Operational Engineers
What's New

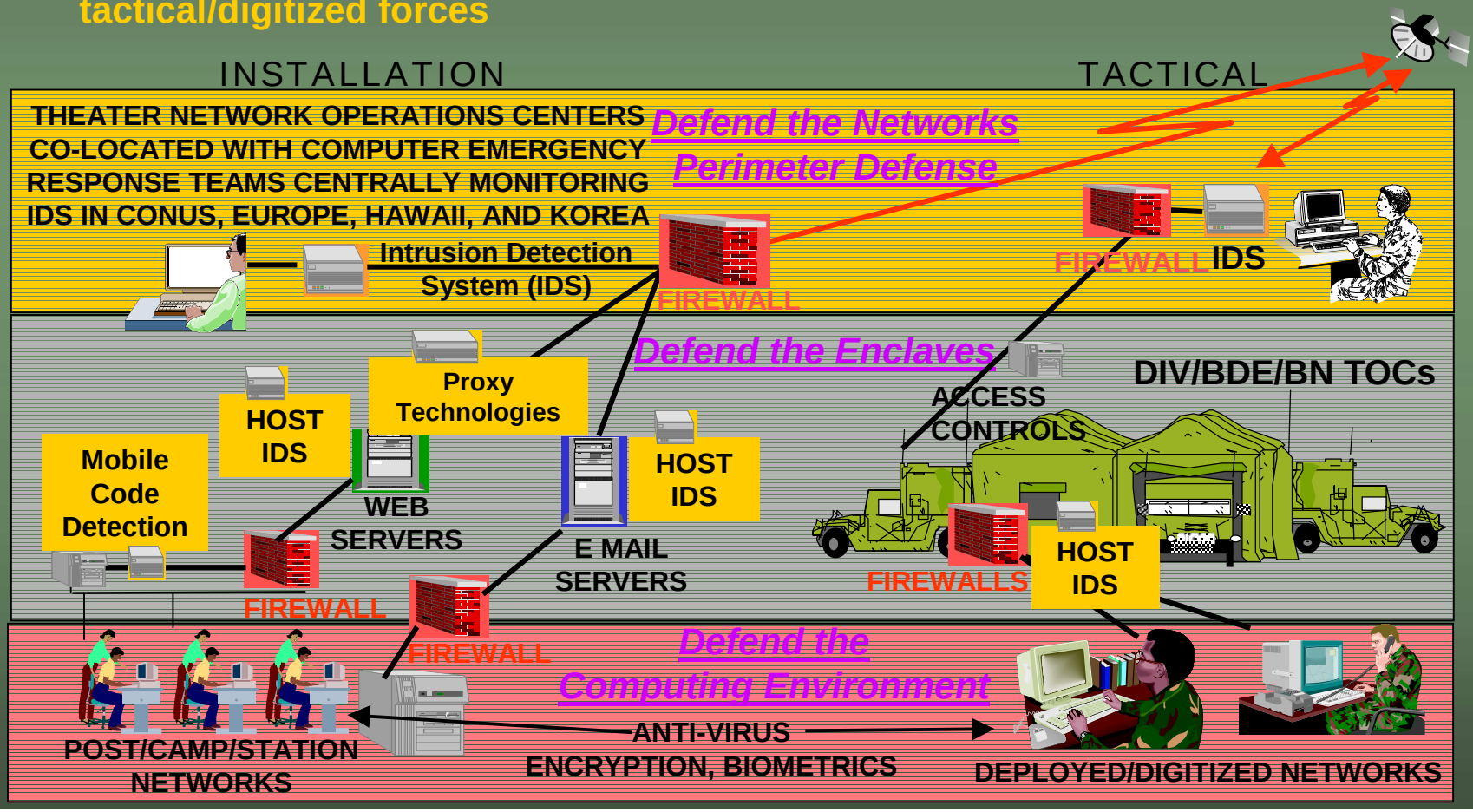
Computer Network Defense



Army Information Assurance

Shapes the Cyber Battle-Space for Future IO Operations

- Establishes effective policies and tactics, techniques, and procedures (TTPs) across the full spectrum of conflict
- Identifies, trains, and retains quality IA personnel
- Inserts state-of-the-art protective technologies into sustaining base and tactical/digitized forces



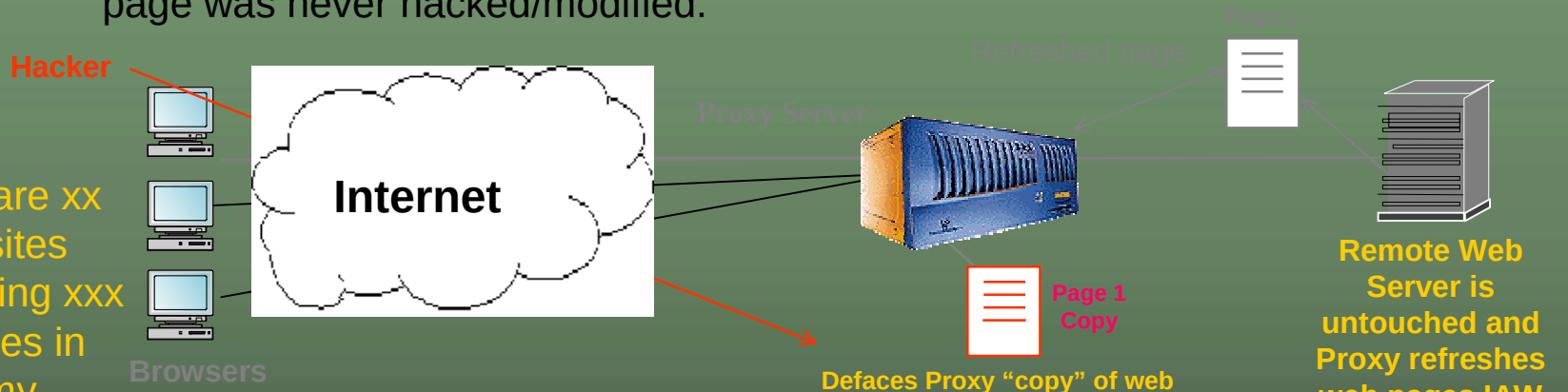
Army Information Assurance Initiatives

(Proxy Technology Protecting the Army's Web Presence to the World)

During Dec 01 – at the height of the Nimda Worm attack, there were 96,274 exploits attempted against Army web servers protected by proxy servers – all were *UNSUCCESSFUL* in defacing a page.

How it works:

If the web page is hacked/modified on the proxy server, the original web page can be used to update the proxy version since the original page was never hacked/modified.



Army Ports and Protocols Registration Process

(Army Ports and Protocols Registration Process)

Challenge

- **Uniform and timely process for requests to "open" protocols and ports at security enabled network devices (i.e. firewalls, security routers, etc.) that supports…**
  - **High system availability across Army and DoD networks**
- **Spans all operational environments and systems that rely on "computer networks" as their transport mechanism**

“Take Aways”

Information Operation & Information Assurance

- **Dynamic & Growing Enterprise**
- **Open to NEW Initiatives**
- **“Do not know what we don’t know…”**